

**INFORMATION SECURITY POLICY**

*Approved by the Governing Council on 22 February 2024*

**ÍNDEX**

<b>1.</b>	<b>APPROVAL AND ENTRY INTO FORCE</b>	<b>3</b>
<b>2.</b>	<b>INTRODUCTION</b>	<b>3</b>
<b>2.1.</b>	<b>Prevention</b>	<b>3</b>
<b>2.3.</b>	<b>Response</b>	<b>4</b>
<b>2.4.</b>	<b>Recovery</b>	<b>4</b>
<b>3.</b>	<b>MISSION OF THE UNIVERSIDAD ROVIRA I VIRGILI</b>	<b>4</b>
<b>4.</b>	<b>BASIC PRINCIPLES</b>	<b>4</b>
<b>5.</b>	<b>INFORMATION SECURITY OBJECTIVES</b>	<b>5</b>
<b>6.</b>	<b>SCOPE</b>	<b>6</b>
<b>7.</b>	<b>ORGANISATION OF INFORMATION SECURITY</b>	<b>6</b>
<b>7.1.</b>	<b>Criteria used for organising information security security</b>	<b>6</b>
<b>7.2.</b>	<b>Information Security Appointees and Bodies</b>	<b>7</b>
<b>7.3.</b>	<b>Responsibilities of the roles associated with the National Security Scheme</b>	<b>8</b>
<b>7.4.</b>	<b>Data Protection Officers</b>	<b>10</b>
<b>7.5.</b>	<b>ICT Security Committee</b>	<b>10</b>
<b>7.6.</b>	<b>ICT Security Office</b>	<b>11</b>
<b>7.7.</b>	<b>Cybersecurity Operations Centre</b>	<b>12</b>
<b>7.8.</b>	<b>Designation procedures</b>	<b>13</b>

<b>7.9. Conflict resolution</b>	<b>13</b>
<b>8. PERSONAL INFORMATION</b>	<b>13</b>
<b>9. STAFF OBLIGATIONS</b>	<b>13</b>
<b>10. RISK MANAGEMENT</b>	<b>13</b>
<b>11. REPORTING OF INCIDENTS</b>	<b>14</b>
<b>12. LEVELS OF THE INFORMATION SECURITY POLICY</b>	<b>14</b>
<b>13. THIRD PARTIES</b>	<b>15</b>
<b>14. CONTINUOUS IMPROVEMENT</b>	<b>15</b>
<b>15. DEROGATION OF PREVIOUS POLICY</b>	<b>15</b>

## 1. APPROVAL AND ENTRY INTO FORCE

Text approved on ..... by agreement issued by the Governing Council of the Universitat Rovira i Virgili.

This "Information Security Policy", hereafter referred to as the "Policy", will be effective from the date of its approval until it is replaced by a new policy.

## 2. INTRODUCTION

The Universitat Rovira i Virgili depends on ICT (Information and Communication Technologies) systems to achieve its objectives. These systems must be managed diligently with appropriate measures to protect them against accidental or deliberate damage that could affect the security of the information processed or the services provided, and they must always have protection against threats or incidents that have the potential to affect the confidentiality, integrity, availability, traceability and authenticity of the information processed and the services provided.

In order to face these threats, a strategy is needed that adapts to changes in the conditions of the environment so as to guarantee the continuous provision of services. This means that the Universitat Rovira i Virgili must apply the security measures required by the National Security Scheme (NSS), continuously monitor its levels of service provision, monitor and analyse the vulnerabilities reported, and prepare an effective response to cyber-incidents to ensure the continuity of the services it provides.

These measures must be followed by all the structures that form part of the University, bearing in mind that ICT security is an integral part of each stage of the system's life cycle, from its conception to its withdrawal and including development or acquisition decisions and operational activities. Security requirements and funding needs must be identified and included in the planning, tendering and bidding processes for ICT projects.

Therefore, for the Universitat Rovira i Virgili, the objective of information security is to protect information and information systems against unauthorised access, use, disclosure, interruption, modification or destruction, thus ensuring the confidentiality, integrity and availability of the information and the continuous provision of services. To do so, the Universitat Rovira i Virgili must act preventively by implementing protection measures, monitoring daily activity to detect any incident and reacting promptly to incidents in order to recover services as soon as possible, in accordance with the provisions of the NSS and by applying the following measures.

### 2.1. Prevention

- To ensure that information and/or services are not damaged by security incidents, the Universitat Rovira i Virgili must implement the security measures established by the NSS, as well as any other additional controls that it has identified as necessary through an assessment of threats and risks. These controls and the security roles and responsibilities of all staff must be clearly defined and documented.
- To ensure compliance with the Policy, the Universitat Rovira i Virgili will:
- Authorise the systems before they go into operation.
- Regularly assesses security, including the analysis of routine configuration changes.
- Request periodic reviews of its security by third parties to obtain independent evaluations.
- Verify that its incident recovery and business continuity measures are functioning

correctly.

### 2.2. *Detection*

The Universitat Rovira i Virgili has to establish operational controls in its information systems in order to detect anomalies in its provision of services and act accordingly in accordance with the provisions of article 10 of the NSS (continuous monitoring and periodic reassessment). The Universitat Rovira i Virgili has to establish mechanisms for detection and analysis so that when there is significant deviation from previously established normal parameters (in accordance with the provisions of article 9 of the NSS, Existence of lines of defence) it is reported to those responsible.

### 2.3. *Response*

The Universitat Rovira i Virgili must:

- Establish mechanisms to respond effectively to security incidents.
- Designate a point of contact for reporting incidents detected at the university and in other organisations.
- Establish protocols for exchanging information relating to the incident. This includes two-way communication with the Computer Emergency Response Teams (CERT).

### 2.4. *Recovery*

In order to ensure the continued provision of its services, the Universitat Rovira i Virgili must have in place the necessary means and techniques to guarantee the recovery of its most critical services.

## 3. MISSION OF THE UNIVERSIDAD ROVIRA I VIRGILI

The purpose of the present Information Security Policy of the Universitat Rovira i Virgili is to establish a baseline of reliability with which the information systems provide their services and safeguard information in accordance with the functional specifications. This baseline reliability must ensure that the information systems function without interruptions or modifications outside the URV's control and without the information reaching the knowledge of unauthorised persons.

The objective of information security is to guarantee the quality of information and business continuity by acting preventively, supervising daily activity and reacting quickly to incidents.

## 4. BASIC PRINCIPLES

The basic principles are fundamental security guidelines that must always be taken into account in any activity related to the use of information assets. The following basic principles are established:

- **Strategic scope:** Information security must have the commitment and support of all the University's management levels so that it can be coordinated and integrated with the rest of the organisation's strategic initiatives to form a coherent and effective whole.
- **Identification of responsibility:** It is necessary to identify the person responsible for the information, the person responsible for the service, who determines the security requirements of the information processed, the person responsible for the system, who is responsible for the provision of the services, and the person responsible for security, who takes decisions to meet the security requirements. When personal data is processed, these

persons or units must coordinate with the data protection officers in order to apply the principles of personal data protection from the outset and by default.

- **Comprehensive security:** Security must be understood as a comprehensive process covering all the technical, human, material and organisational elements related to ICT systems. It should not involve sporadic actions or avoid any specific action or joint treatment. Information security must be considered as part of normal operations, and must be present and applied from the initial design of ICT systems.
- **Risk Management:** Risk analysis and management must be an essential part of the safety process. Risk management must make it possible to maintain a controlled environment and minimise risks to acceptable levels. The reduction of these levels must be achieved through the deployment of security measures, which must strike a balance between the nature of the data and the processes, the impact and likelihood of the risks to which they are exposed and the effectiveness and cost of the security measures. In assessing risk in relation to data security, the risks arising from the processing of personal data must be taken into account.
- **Proportionality:** The protection, detection and recovery measures established must be proportional to the potential risks and the critical nature and value of the information and services that they are intended to protect.
- **Continuous improvement:** Security measures must be periodically reassessed and updated to adapt their effectiveness to the constant evolution of risks and protection systems. Information security must be monitored, reviewed and audited by qualified, trained and dedicated personnel.
- **Default security:** Systems must be designed and configured to ensure a sufficient default level of security.

## 5. INFORMATION SECURITY OBJECTIVES

The Universitat Rovira i Virgili has the following information security objectives:

- **To guarantee the quality and protection of the information:** the information must be credible, precise, objective and trustworthy.
- **To raise awareness and provide training:** Users must be fully aware of information security.
- **To manage information assets:** The university's information assets must be inventoried and categorised, and must be associated with a person in charge.
- **To provide security linked to people:** The necessary mechanisms must be put in place so that anyone who accesses the URV's information assets is fully aware of their information security responsibilities, thereby reducing the risk of improper use.
- **To provide physical security:** Information assets must be located in secure areas, protected by physical access controls appropriate to their level of criticality. The information systems and assets contained in these areas will be sufficiently protected against physical or environmental threats.
- **To securely manage communications and operations:** The necessary procedures must be established in order to manage effectively the security, operation and updating of ICTs. The information that is transmitted through communication networks must be

adequately protected by means of mechanisms that guarantee security, taking into account the information's level of sensitivity and criticality.

- To control access: Access to information assets by users, processes and other information systems must be limited by implementing identification, authentication and authorisation mechanisms in accordance with the criticality of each asset. Furthermore, access to and use of the system must be recorded to ensure traceability and appropriate use, in accordance with the organisation's activities.
- To acquire, develop and maintain information sources: Information security aspects must be considered in all phases of the life cycle of information systems in order to guarantee their security by default.
- To manage safety incidents: Appropriate mechanisms must be implemented for the correct identification, recording and resolution of safety incidents.
- To guarantee the continuous provision of services: Appropriate mechanisms must be implemented to ensure the availability of information systems and maintain the continuity of business processes, in accordance with the service level needs of users.
- To protect personal data: The appropriate technical and organisational measures must be adopted to deal with the risks generated by the processing of personal data and to comply with legislation on the protection of personal data and security.
- Compliance: The necessary technical, organisational and procedural measures must be adopted to comply with the legal regulations in force in the field of information security.

## 6. SCOPE

The present Policy applies to the information systems of the Universitat Rovira i Virgili and their use in the exercise of its competences and to all users with authorised access, whether or not they are employees and regardless of the nature of their legal relationship with the university. All users are obliged to know and comply with this Information Security Policy and the Security Instructions that derive from it, and it is the responsibility of the ICT Security Committee to provide the necessary means to ensure that the information reaches the staff concerned.

## 7. ORGANISATION OF INFORMATION SECURITY

### *7.1. Criteria used for organising information security security*

When organising its information security, the Universitat Rovira i Virgili must take into account the provisions of the aforementioned Royal Decree 311/2022, of 3 May, which regulates the National Security Scheme (NSS), the guidelines established in the document CCN-STIC-801 "Responsibilities and Functions in the NSS", and specifically the guidelines in the document CCN-STIC-881 "Guide for Universities adapting to the NSS" and the CCN-STIC-881A guide "Specific complementary university profile".

Consequently, in the light of these provisions and guidelines, the Universitat Rovira i Virgili must:

- Appoint people to the following security roles: Services Officers, Information Officers, Security Officer, System Officer and Data Protection Officer.
- Create a consultative and strategic body for taking decisions on information security. This body must be constituted as a collegiate body and will be called the

Information Security Committee. It will be chaired by a natural person who will be formally responsible for its actions.

### *7.2. Information Security Appointees and Bodies*

Within the framework of the NSS, at the Universitat Rovira i Virgili, the appointees and bodies concerned with Information Security, are the:

- System Officer: Director of the Computer Resources and Information Technology Service of the Universitat Rovira i Virgili.
- Security Officer: The Security Officer can be an internal or external figure, at executive level, formally appointed by the rector. The Security Officer may not be a single-person governing entity of the university and must not have any responsibility for the provision of ICT services, nor must they be in a relationship of hierarchical inferiority to the System Officer (or vice versa).
- Information Officers and Services Officers of the University: Heads and managers of the university's various administrative bodies and units.
- ICT Security Committee:
  - o Chair: Rector or delegated individual.
  - o Members:
    - Permanent members:
      - Secretary: Information and Communication Technologies Officer from the management team.
      - General Manager or delegated individual.
      - System Officer.
      - Information Security Officer.
      - The Data Protection Officer (who can speak but not vote)
    - Non-permanent members:
      - Members of the Governing Council, who will be convened by the chair depending on the issues that need to be dealt with. They will have the right to speak but not to vote.
      - Information Officers and Services Officers of the university, who will be convened by the chair depending on the issues that need to be dealt with. They will have the right to speak but not to vote.
      - The ICT Security Committee may call for the presence at its meetings of other university representatives as well as external specialists from the public, private and/or academic sectors, whose presence may be necessary or advisable due to their experience or connection with the issues that need to be dealt with. They will have the right to speak but not to vote.

The Information Officers and Security Officers will be convened by the chair depending on the issues that need to be dealt with.

The Data Protection Officer will have the right to speak but not to vote in the meetings of the Information Security Committee whenever the meetings concern issues relating to

personal data processing and whenever Data Protection Officer's participation is required. In these cases, when an issue is put to vote, the opinion of the Data Protection Officer must always be recorded in the minutes.

The secretary of the Committee shall convene and record the minutes of the meetings of the Security Committee. The chair of the Security Committee may permit the attendance at its meetings of any persons as may be considered appropriate to act in the capacity of advisors.

### *7.3. Responsibilities of the roles associated with the National Security Scheme*

#### 7.3.1 Information Officers and Services Officers

The duties of the Information Officers and Services Officers are to:

Establish and submit for approval to the Information Security Committee the security requirements applicable to information (information security levels) and services (service security levels), within the framework established in Annex I of the RD NSS. They may request a proposal from the Security Officer whilst taking into account the opinion of the System Manager.

Rule on the right of access to information and to services.

Accept the levels of residual risk affecting information and services.

Notify the Security Officer of any change in the information and services for which they are responsible, especially the incorporation of new services or information under their responsibility. The Security Officer must report these changes to the Information Security Committee at its next meeting.

#### 7.3.2 Security Officer

The duties of the Security Officer are to:

Maintain and verify the appropriate level of security of the information managed and the electronic services provided by the information systems.

Promote information security training and awareness.

Appoint individuals responsible for carrying out risk analyses and Declarations of Applicability, identifying security measures, determining the necessary configurations, and writing the documentation for the system.

Provide advice on determining the System Category, in collaboration with the System Officer and/or the ICT Security Committee.

Participate in the preparation, implementation and validation of security improvement plans and, if necessary, continuity plans.

Manage external and internal revisions of the system.

Manage certification processes.

Submit to the Security Committee the approval of changes and other system requirements.

Approve the security procedures that form part of the Regulatory Map (which do not fall within the remit of the Security Committee) and inform the Security Committee of any modifications made during the current period.

### 7.3.3 System Officer

The duties of the System Officer are to:

- Develop, operate and maintain the information system throughout its life cycle, drawing up the necessary operating procedures.
- Define the topology and management of the Information System, establishing the criteria for its use and the services available in it.
- Stop access to information or provision of services if they become aware that these have serious security deficiencies.
- Ensure that specific security measures are adequately integrated into the general security framework.
- Provide advice to determine the category of the system, in collaboration with the Security Officer and/or the Information Security Committee.
- Participate in the preparation and implementation of security improvement plans and, if necessary, continuity plans.
- Carry out, if necessary, the functions of the system security administrator, which are to:
  - o Manage, configure and update, if necessary, the hardware and software on which the security mechanisms and services are based.
  - o Manage the authorisations (in particular the privileges) granted to users of the system, and monitor the activity carried out in the system to check that it corresponds with what is authorised.
  - o Approve changes to the current configuration of the Information System.
  - o Ensure strict compliance with the established security controls.
  - o Ensure the application of the procedures approved for managing the information system.
  - o Supervise the installation, modification and improvement of hardware and software to ensure that security is not compromised and that at all times they comply with the relevant authorisations.
  - o Use security event management tools and technical audit mechanisms to monitor security status.
  - o Inform the Security Officer of any security-related anomaly, compromise or vulnerability.
  - o Collaborate in the detection, investigation and resolution of security incidents.

When the complexity of the system justifies it, the System Officer may appoint any additional individuals to work on the system that they consider necessary. These individuals will answer directly to the System Officer and will be responsible in their area for all those actions that are delegated to them. In the same way, the System Officer may also delegate other specific functions for which they are responsible.

#### 7.4. Data Protection Officers

The duties of the Data Protection Officers are to:

- Inform and advise the Universitat Rovira i Virgili, and the users who deal with data processing, regarding their obligations under the current legislation on data protection.
- Supervise compliance with the security regulations and the internal policies of the Universitat Rovira i Virgili regarding matters of personal data protection. This includes supervising the assignation of responsibilities, the awareness and training of staff involved in data processing operations, and the auditing process.
- Provide any advice requested regarding the impact assessment relating to the protection of personal data and to supervise its application.
- Carry out all other duties established in the regulations governing personal data protection and security.

#### 7.5. ICT Security Committee

The ICT Security Committee must:

- a) Have at all times up-to-date information regarding the set of documentation that regulates the NSS Compliance Certification, including the rules for accreditation and certification, guidelines, manuals, procedures and technical instructions.
- b) Have at all times up-to-date information regarding the list of accredited Certification Bodies and certified public and private organisations.
- c) Have at all times up-to-date information regarding the list of security certification schemes with which the Public Administration has established agreements for the mutual recognition of certificates.
- d) Propose guidelines and recommendations, which will be included in the corresponding minutes of the Committee's meetings, to which the chair of the Committee must provide a full response.
- e) Coordinate the efforts of the different areas in the field of information security to ensure that they are consistent and aligned with the agreed strategy and to avoid duplication.
- f) Address the information security concerns of the university community and regularly report on the status of information security to the Management.
- g) Resolve conflicts of responsibility that may arise between the different officers and/or between structures, and to escalate those cases in which it does not have sufficient authority to decide.
- h) Advise on information security matters, whenever required to do so.
- i) Review the Information Security Policy prior to approval by the Governing Council.
- j) Approve the Instructions regarding the Use of Electronic Media by all staff.
- k) Approve the Map of Security Instructions for the implementation of the NSS.

Periodicity of meetings and adoption of agreements:

1. The ICT Security Committee will meet at least once a quarter during the NSS Adaptation Project in order to monitor and assess its progress.
2. Once the services provided by the University have obtained the NSS Compliance Certification, the ICT Security Committee will meet at least every six months, although the number of meetings may increase if so required.
3. In all cases, meetings shall be convened by the chair, through the secretary, at the chair's request or at the request of the majority of the permanent members.
4. Decisions must be adopted by a qualified majority of 3/4 of the members attending with the right to vote.

#### *7.6. ICT Security Office*

The ICT Security Office is constituted within the cybersecurity governance structure. Its competences are related to the following areas of work: adaptation to the NSS, risk management, continuous assessment and improvement, security in interconnections and connectivity and other related or concordant functions.

The ICT Security Office consists of:

- The Director of the ICT Security Office, appointed by the ICT Security Committee and acting as a liaison, this role is taken by the Security Officer or delegated individual.
- The Secretary of the ICT Security Office, appointed by the ICT Security Committee, at the proposal of the members of the Security Office.
- All security specialist administrators who the Security Officer determines to be necessary.

The ICT Security Officer will coordinate with the Data Protection Officer and all Service and Information Officers that the Security Officer determines to be necessary, depending on the issues to be dealt with.

Among others that may be entrusted to it by the ICT Security Committee, the functions of the ICT Security Office are to:

- a) Manage and operate the security of the NSS Compliance Adaptation, Implementation and Management Project, and to carry out the analysis and management of risks, exploitation, documentation and maintenance.
- b) Draft and present proposals to the ICT Security Committee. It has to draft aspects relating to cybersecurity so they can be submitted to the Committee.
- c) Promote the continuous improvement of the information security management system. To this end, it will be responsible for:
  - o Drawing up (and regularly reviewing) the Information Security Policy and submitting it to the ICT Security Committee for review and subsequent approval by the Governing Council.
  - o Drawing up the Information Security documentation for approval by the Security Officer, with the knowledge of the Security Committee.
  - o Verifying the information security procedures and the rest of the documentation for approval.

- o Drawing up training programmes aimed at training and raising staff awareness of information security and data protection, in coordination with the data protection officers.
- o Drawing up and approving the information security training and qualification requirements for administrators, operators and users.
- o Proposing plans for improving information security, with the corresponding budget allocation, and prioritising actions in the area of security when resources are limited.
- o Monitoring the main residual risks and recommending possible actions to be taken in this respect.
- o Promoting periodic audits of the NSS and the RGPD to verify the university's compliance with its information security and data protection obligations.

Periodicity of meetings and adoption of agreements:

1. The director of the ICT Security Office will call its members to working meetings and will record the decisions reached at these meetings, which must be reported to the ICT Security Committee for approval.
2. The Office may convene plenary sessions or working groups to analyse and make specific proposals. If necessary, proposals submitted to the ICT Security Office must be subject to analysis, debate and approval by the ICT Security Committee.
3. It will meet at least once a quarter and always before the ICT Security Committee meeting is held.

#### *7.7. Cybersecurity Operations Centre*

The Cybersecurity Operations Centre provides cybersecurity services to monitor and detect threats to the day-to-day operation of ICT systems, while improving the system's ability to respond to any attack.

Functions

The functions of the Cybersecurity Operations Centre will be to:

- Watch over and monitor the security of the systems and of the defence devices by using planned interfaces or by installing the necessary probes.
- Analyse and correlate security events and system activity logs.
- Carry out security operations on defence devices.
- Set up a Security Incident Response Team. This team must have a person in charge and be responsible for monitoring the management of security incidents and recommending possible actions to improve security.
- Implement an Early Warning System to provide security alerts for corporate networks and for the system's internet connections.
- Carry out vulnerability remediation by identifying and applying fixes and patches to applications and services.
- Carry out digital forensic and security analyses.
- Implement and manage cyber-surveillance services in order to anticipate cyber-threats.

The functions of the Cybersecurity Operations Centre will be carried out wholly or in part by the ICT Resources Service in collaboration with the ICT Security Office

#### *7.8. Designation procedures*

The Rector of the Universitat Rovira i Virgili will constitute the Information Security Committee and appoint its members and the officers identified in this Policy.

#### *7.9. Conflict resolution*

Any conflict between the various officers will be resolved by their hierarchical superior. If this is not possible, the conflict will be resolved by the URV's Information Security Committee.

### **8. PERSONAL INFORMATION**

The Universitat Rovira i Virgili will only collect and process the personal data that is necessary and relevant to the scope and purposes for which they were obtained. Likewise, it will adopt the technical and organisational measures necessary to comply with data protection regulations.

The Universitat Rovira i Virgili will publish its Privacy Policy on its website.

### **9. STAFF OBLIGATIONS**

All Universitat Rovira i Virgili staff included within the scope of the NSS must attend one or more awareness sessions on security and data protection. An ongoing awareness programme should be established for all staff, particularly new recruits.

Persons responsible for operating or administering information systems must receive training in the safe use of the systems to the extent that they need it to carry out their work. Staff must receive compulsory training before taking on a responsibility, regardless of whether it is their first assignment or they are changing to a new role or new responsibilities.

### **10. RISK MANAGEMENT**

All systems governed by this Information Security Policy will be subject to a risk analysis in order to assess the threats and risks to which they are exposed. This analysis will be repeated:

- At least once a year.
- When the information and/or services change significantly.
- When a serious security incident occurs or serious vulnerabilities are detected.

The Security Officer will be responsible for carrying out the risk analysis, identifying shortcomings and weaknesses and reporting these to the Information Security Committee.

The Information Security Committee has to ensure the availability of resources to meet the security needs of the different systems, promoting horizontal investments.

The risk management process will consist of the following phases:

- Categorisation of systems.

- Risk analysis.
- Selection by the Information Security Committee of the security measures to be applied, which must be proportional to the risks identified.

The phases of this process will be carried out in accordance with the provisions of Annexes I and II of Royal Decree 311/2022, of 8 January, and following the rules, instructions, CCN-STIC guidelines and recommendations for its application drawn up by the CCN.

In particular, as a general rule, a recognised risk analysis and management methodology will be used to carry out risk analysis.

## 11. REPORTING OF INCIDENTS

In accordance with article 33 of RD 311/2022, of 3 May/January, the Universitat Rovira i Virgili will notify the National Cryptological Centre of any incidents that have a significant impact on the security of the information handled and the services provided in relation to the categorisation of systems included in Annex I of the aforementioned legal framework.

## 12. LEVELS OF THE INFORMATION SECURITY POLICY

This Information Security Policy will be complemented by documentation and security recommendations (security instructions, technical security procedures, reports, records and electronic evidence). The Information Security Committee will be responsible for its annual review and/or maintenance and, if necessary, will propose improvements to it.

The regulatory framework on information security will have three levels, namely scope of application, technical detail and mandatory compliance, so that a regulation from a given level draws its authority from higher level regulations. These regulatory levels are as follows:

- a) First regulatory level: this consists of the present Information Security Policy, the Internal Instructions on the Use of Electronic Media and the general security guidelines applicable to the university bodies or units that are subject to these documents.
- b) Second regulatory level: this consists of the security regulations derived from the previous regulations.
- c) Third regulatory level: this consists of procedures, guides and technical instructions. These are documents that, in accordance with the Information Security Policy, determine which actions or tasks need to be carried out for a given process.

The highest body of the Universitat Rovira i Virgili (Governing Council) is responsible for approving the Information Security Policy and the Internal Instructions on the Use of Electronic Media; the Information Security Committee is the body responsible for approving the remaining documents, and is also responsible for their dissemination so that the affected parties are aware of them.

Likewise, the present Information Security Policy complements the Universitat Rovira i Virgili's Privacy Policy in terms of data protection.

The security documentation and, in particular, the Information Security Policy and the

Internal Instructions on the Use of Electronic Media, will be available to and known by all members of the university, especially to those who use, operate or administer information and communication systems. It will be available for consultation on the Intranet and in paper format, and will be kept by the Office of the Secretary General.

### **13. THIRD PARTIES**

When the Universitat Rovira i Virgili provides services to or processes information from other bodies, these other bodies will be required to comply with this Information Security Policy. Channels will be established to report on and coordinate the respective Information Security Committees and action procedures will be established to react to security incidents.

When the Universitat Rovira i Virgili uses third-party services or provides information to third parties, it will inform them of this Security Policy and of the security documentation that affects these services or information. The third party will be subject to the obligations established in this documentation, and may develop its own operational procedures to meet them. Specific procedures for reporting and resolving incidents will be established. The Universitat Rovira i Virgili will ensure that third-party personnel are security-aware to at least the same level as that established in the present Security Policy.

If any aspect of this Information Security Policy cannot be satisfied by a third party in the manner required in the preceding paragraphs, the Security Officer must issue a report outlining the risks involved and how to deal with them. The information and services officers affected must approve this report before proceeding any further.

### **14. CONTINUOUS IMPROVEMENT**

Information security management is a process that requires constant updating. Changes in the organisation, threats, technologies and/or legislation are examples of where continuous improvement of the systems is required. For this reason, it is necessary to implement a permanent process that, among other actions, will:

- a) Review the information security policy.
- b) Review services, information and categorisation.
- c) Undertake an annual risk analysis.
- d) Undertake internal and, when necessary, external audits.
- e) Review security measures.
- f) Review and update rules and procedures.

### **15. DEROGATION OF PREVIOUS POLICY**

The present Information Security Policy replaces the Information Security Policy approved by the Governing Council on 23 October 2018 and subsequently amended on 23 October 2019.